State of Colorado

Information and Technology **Management Code**

Version 1.0

Rules and regulations to control purchases by state agencies and to be used in approving or rejecting agency procurements

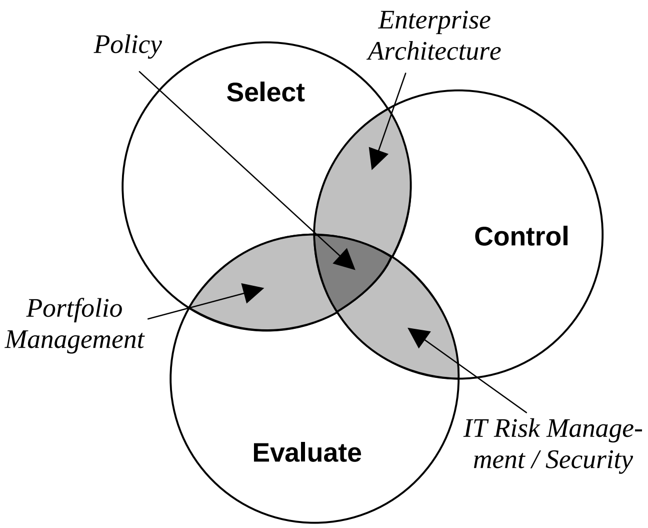
Effective March 2, 2006

Commission on Information Management (IMC)
Governor’s Office of Innovation and Technology (OIT)

Table of Contents

General Statement

A central tenet of the State's e-Government Framework – an approach selected by both the Governor's Office of Innovation and Technology (OIT) and the Commission on Information Management (IMC) to coordinate and direct the use of communication and information resources and technologies by state agencies – is the universally accepted select/control/evaluate model. It provides a systematic method for agencies to minimize risks while maximizing the returns of investments in communication and information resources technologies.



Policy – a set of principles, communicated through governance documents, that constitute the core framework (vision, goals, strategies) to be used as a guide for defining organizational success. "*Are we doing the right things*?"

Select – to screen and rank each existing and potential new investment; choose those that best support the organization's mission needs (identify gaps; compare alternative risks and returns; decide on investments' cost, schedule, and scope).

Enterprise Architecture – a set of aligned business and IT reference models designed to facilitate cross-organizational analysis, differentiate specialized, shared, and common services, and guide collaboration (standards). "*Are we doing them the right way*?"

Control – to manage investments throughout their entire lifecycle to ensure they continue to meet mission needs at expected levels of cost and risk (monitor; take corrective actions).

IT Risk Management / Security – a set of techniques to measure, monitor, and control the possibility a particular threat will exploit a particular vulnerability with a particular harmful result (best practices; dashboards). "*Are we getting them done well*?"

Evaluate – to measure actual versus expected results (assess projects' impact on mission performance; identify modifications needed to projects; revise investment management process).

Portfolio Management – a set of investments purposefully prioritized and balanced to best achieve the organization's mission needs (metrics; scorecards). "*Are we getting the benefits*?"

The Commission on Information (IMC) has chosen to mirror this framework in the structure of the State Information and Technology Management Code (i.e., IT Management Rules).

The purpose, statutory authority, definitions, applicability, responsibility and administrative hardship outlined on the next page are applicable to each of the rules which compose the State's Information and Technology Management Code and should be attached to any rule that is separated from this Code.

Purpose

The purpose of these IT management rules is to coordinate and direct the use of communication and information resources and technologies by state agencies and to provide as soon as possible the most cost-effective and useful exchange of information both among the various state agencies as well as from government to the people of Colorado. Furthermore, these rules are intended to facilitate the oversight of strategic planning and setting policy for the state's communications and information systems as well as assuring continuity in communications and planning and controlling the state's investment in information systems. In furtherance of these purposes, these rules are to control purchases by state agencies and to be used in approving or rejecting agency procurements. This is incorporated as a reference into each of these State IT Management Rules.

Statutory Authority

Colorado's Governor and General Assembly partnered, through legislation and the Colorado Revised Statutes, to create both the Governor's Office of Innovation and Technology (OIT) and the Commission on Information Management (IMC). Part 1 of C.R.S. Title 24, Article 37.5 outlines the duties and responsibilities of the OIT. Part 2 of C.R.S. Title 24, Article 37.5 outlines the powers and duties of the IMC. Rule-making authority is granted to the IMC as specified in both C.R.S. 24-37.5-202 (1)(d) and C.R.S. 24-37.5-203.5 (7). These are incorporated as a reference into each of these State IT Management Rules.

Definitions

Those definitions contained in the above referenced IMC and OIT portions of the Colorado Revised Statutes – including C.R.S. 24-37.5-102 – are incorporated into each of these State IT Management Rules.

Applicability

As directives of the IMC, these State IT Management Rules are applicable to all state agencies as defined in C.R.S. 24-37.5-101 (5) – every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions, but not state-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof. Additionally, these rules apply to all expenditures technologies and technology resources as defined by C.R.S. 24-37.5-102 (1) and (2) regardless of funding source. This is incorporated as a reference into each of these State IT Management Rules.

Responsibility

It is the responsibility of the chief executive officer of each state agency to ensure compliance with these State IT management rules. This is incorporated as a reference into each of these State IT Management Rules.

Administrative, financial, or business impact

Should any of these State IT Management Rules create adverse administrative, financial, or business impact on a state agency, a formal written request for exception and/or alternative policy may be submitted by the state agency to the Chair of the IMC with notification to the state agency's chief executive officer. Exceptions will be reviewed no less frequently than once per month. When an exception is granted, the resulting explicit approval shall identify the scope and effective period of said exception. This is incorporated as a reference into each of these State IT Management Rules.

Exceptions

Exceptions granted to agencies by the IMC/OIT in an explicit approval as part of a formal IMC/OIT process are recognized as approved exceptions in other formal IMC/OIT processes. Additionally, see "administrative, financial, or business impact" section above. This is incorporated as a reference into each of these State IT Management Rules.

Chapter 1

Select

Management Rule	**Number**
IT Management Principles	1-1
Annual IT Planning	1-2
Minimum IT Architecture Standards	1-3

Rule 1-1
IT Management Principles

Authority

C.R.S. 24-30-1603 (3)(b) – Each agency designate a CIO (DPA)
C.R.S. 24-37.5-101 (1)(g) – Legislative declaration (OIT)
C.R.S. 24-37.5-202 (1)(a) – Assure agency alignment with State plan (IMC)
C.R.S. 24-37.5-202 (1)(b) – Assess status of current state (IMC)
C.R.S. 24-37.5-202 (1)(g) – Study needs of state agencies (IMC)
C.R.S. 24-37.5-203 (1)(b) – Review existing portions of the Statewide infrastructure (IMC)
C.R.S. 24-37.5-203 (1)(e) – Oversee on-going use of statewide infrastructure (IMC)

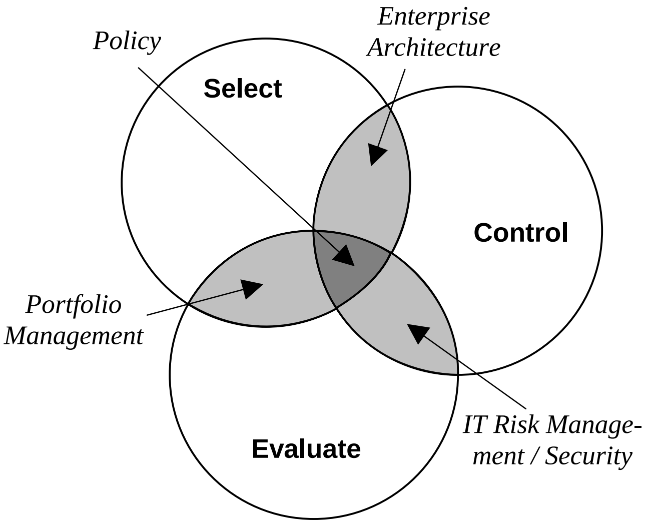
Rule

It is a directive of the Commission on Information Management (IMC), that the information and technology (IT) management principles of the State shall be based:

- First, on the two (2) supreme policies set forth by the governor and general assembly in statute (CRS 24-37.5-101) – It is the policy of this state:
    - to coordinate and direct the use of communication and information resources technologies by state agencies; and
    - to provide as soon as possible the most cost-effective and useful retrieval and exchange of information both within and among the various state agencies and branches of government and from the state agencies and branches of government to the people of Colorado;

<table>
<tr><td><b>Vision</b></td><td colspan="4">Provide the most cost-effective and useful retrieval and exchange of information both among agencies and from government to the citizens</td></tr>
<tr><td><b>Goals</b></td><td colspan="2">Improve interactions between government and its customers (front office)</td><td colspan="2">Enhance IT service delivery and promote operational excellence (back office)</td></tr>
<tr><td><b>Strategies</b></td><td>Policy Structure</td><td>Enterprise Architecture</td><td>Risk Management</td><td>Portfolio Management</td></tr>
</table>

- Second, on the Select/Control/Evaluate model;



- Third, that all agency investments in communication and information resources and technologies – and all associated selection, control, and evaluation activities – shall be coordinated through the agency's designated chief information officer.

The chief information officer of each agency shall annually report to the IMC/OIT as to the current status of and progress toward the agency's compliance with IMC plans, policies, and directives.

The report form, content, and due date shall be determined by the IMC, in consultation with agency chief information officers.

Rule 1-2
Annual IT Planning

Authority

C.R.S. 24-37.5-106 (1)(b) – Require state agencies to submit plans (OIT)
C.R.S. 24-37.5-106 (1)(e) – Effective management of IT investments (OIT)
C.R.S. 24-37.5-106 (1)(i) – Efficient exchange of information and technology (OIT)
C.R.S. 24-37.5-202 (1)(b) – Assess current of systems (IMC)
C.R.S. 24-37.5-202 (1)(g) – Study needs of state agencies (IMC)
C.R.S. 24-37.5-203 (1)(b) – Review existing portions of statewide infrastructure (IMC)
C.R.S. 24-37.5-203 (1)(e) – Oversee on-going use of statewide infrastructure (IMC)

Rule

It is a directive of the Commission on Information Management (IMC), that all state agencies shall submit regularly on at least an annual basis, to the IMC/OIT, an information and technology plan, which includes:

- IT system inventory
- financial, human, physical assets
- IT portfolio
- compliance with IMC Plans, policies, and directives
- needs
- current State
- trends
- statewide communications and information infrastructure
- procurements
- architecture

The documentation form, content, and due date(s) shall be determined by the IMC, in consultation with agency chief information officers.

Rule 1-3

Minimum IT Architecture Standards

Authority

C.R.S. 24-37.5-106 (1)(i) – direct establishment of statewide standards (OIT)
C.R.S. 24-37.5-202 (1)(c) – develop an approach for statewide compatibility (IMC)
C.R.S. 24-37.5-203 (1)(a) – develop and implement requirements for statewide infrastructure (IMC)

Rule

Technical standards are essential to the development and management of a statewide communication and information infrastructure that provides the most cost-effective and useful exchange of information both among the various state agencies and from government to the people of Colorado

This rule consists of two basic components: a body of technical standards and a migration strategy for compliance.

I. A body of technical standards:

It is a directive of the Commission on Information Management (IMC), that the following stable body of industry standards shall represent the minimum IT standards for the State of Colorado.

7.1 Network

A secure, well-organized network that provides reliable connectivity and performance, is required for a web services architecture. See section 7.8 – Security, for additional security requirements.

7.1.1 IP Network

All State computers (desktop, server, mainframe) must be accessible via an IP network.

7.1.2 IP Address Allocation

IP address blocks must be centrally managed for the Enterprise. IP addresses must be allocated geographically following standard sub-netting rules. Each geographical region should aggregate to a single route.

7.1.3 Local Network

Local, un-routable, internal IP addresses that conform with RFC 1918, shall be used on end user devices, to the greatest extent possible.

7.1.4 Routing

State Networks must use a standards based Interior Gateway Routing protocol (IGP) to connect to the MNT. Acceptable protocols are OSPF, EIGRP and RIPv2.

Multi-Protocol Label Switching (MPLS) must be used in the State WAN to provide logical separation of network traffic.

7.1.5 Domain Name Services (DNS)

DNS names registration must be centrally managed and administered. Domain name servers must be redundant and geographically distributed. Machines will be accessed via DNS names to the greatest extent possible.

7.1.6 Reverse Proxy

All State Web servers must utilize reverse proxy servers or virtual IP load balancing technologies. See Figure 7.8.5 - Three Firewall DMZ for a graphical representation of the placement of a reverse proxy server.

7.1.7 Dynamic Host Control Protocol (DHCP)

DHCP must be used for all desktop, laptop, and remote systems. Fixed IP addresses shall only be used for network devices and servers.

7.1.8 VPN (Virtual Private Networking)

Remote access to internal state computational resources must only be provided through secure VPN connections. These connections shall require three (3) element authentication, as a minimum (e.g. an identifier – username, something you know – password, something you have – securid code). these connections must provide encrypted exchange of information through the entire life of the connection.

7.1.8.1 Remote Access VPN

Access VPNs encompass analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable. access to internal state computational resources may only be provided through secure VPN connections.

7.1.8.2 Site-to-Site VPN

Network nodes requiring secure connectivity between themselves and their organizational hub, or where secure connectivity over the Internet is more cost effective and efficient than private WAN connectivity.

7.1.8.3 Extranet VPN

Links between customers, suppliers, partners, or communities of interest to the State Intranet over a shared infrastructure may be provided through secure VPN connections.

7.1.9 Firewall

All State computers must be protected from public access through the use of stateful firewalls. These firewalls must follow the philosophy to deny all access except those protocols, ports, and addresses that are explicitly permitted. Firewall policies shall be clearly documented, reviewed, and updated annually.

7.1.10 Wireless Access Points

No wireless access points or bridges shall be allowed to connect to the State's network without providing:

- 802.1X authentication & authorization for access,
- WEP based encryption, and,
- a non-broadcast SSID.

No wireless Access points are allowed to connect to Data Center network segments.

7.1.11 Network Administrator Security

Default accounts that provide administrator or "super user" privileges on network equipment shall be protected.

7.1.11.1 Default Administrator Passwords

Default administrator passwords shall be changed on installation.

7.1.11.2 Administrator Passwords Strongly Formed

Administrator or super-user passwords shall be strongly formed.

- The password must contain at least one number, one lower case character and one uppercase character.
- The password cannot contain any dictionary word greater than or equal to four (4) characters.
- The password cannot be changed to any of the three (3) previous passwords.
- The password must be at least eight (8) characters long.

7.1.11.3 Administrator Passwords Changed Every 90 Days

All administrative passwords shall be changed at least every ninety (90) days, and on departure of any person with knowledge of those passwords.

7.1.11.4 Administrator Password Storage

Administrative passwords shall not be stored anywhere on the file system in text readable format; this includes operational batch scripts, application programs and password files.

7.1.11.5 Log Failed Admin Access Attempts

All failed attempts to gain access to user accounts with administrative privileges shall be logged and reviewed at least weekly.

7.2 Datacenter

The State has a duty to secure the Public's data and provide for its availability to continually perform the State's business. All data of record stored by the State, must be contained in a clearly identified datacenter. Each datacenter must provide:

a) Datacenter Operational Services
b) Environmentals (Power, HVAC, Fire)
c) Network (bandwidth, utilization, latency, redundancy)

d) Security (physical, network)
e) Backup / Restore Capabilities and Services
f) Disaster recovery

7.2.1 Datacenter Operational Services

Every State datacenter must provide a description of the datacenter operational services provided. On-site vs. off-site support must be clearly identified

7.2.2 Datacenter Environmentals

Every State datacenter must provide controlled environmentals to include: a) conditioned and/or uninterruptible power, b) heating and cooling, and c) fire suppression.

7.2.3 Datacenter Network Access

Every State datacenter must provide network access for mission critical Enterprise data. Network access shall be characterized by bandwidth, utilization, latency and redundancy.

7.2.4 Datacenter Physical Security

Every State datacenter must provide physical security that limits access. This must constitute the second layer of physical access between the public and State owned resources.

7.2.5 Datacenter Network Security

Every State datacenter must provide network security as specified in Section 7.8 - Security.

7.2.6 Datacenter Backup

All State computers (desktop, server, mainframe) must have system, application, and data backup plans and procedures documented. The plans and procedures shall be reviewed and updated annually. These plans must include: 1) periodic backups, 2) periodic movement of backups to offsite storage, 3) periodic recovery testing.

7.2.7 Datacenter Disaster Recovery

A disaster recovery plan must be created for each Department or Agency's computational resources (desktop, server, mainframes, network). The plan must include a business case showing the impact to the State and it's constituents. The plan shall be reviewed and updated annually.

7.3 Web Access

A major goal for the State is to provide one-stop customer service. Internet standards provide a sound technical foundation for that goal. These originate in standards bodies and exist to ensure interoperability between different technologies and are supported by multiple vendors.

Another goal of the State is 24 x 7 service availability. Technologies inherent in web infrastructure are commonplace in the web services market today. Web applications can be easily spread across multiple application servers. If one server fails, another server takes over for it. An edge server can dispatch the browser requests across as many servers as necessary. This provides for 24 x 7 availability.

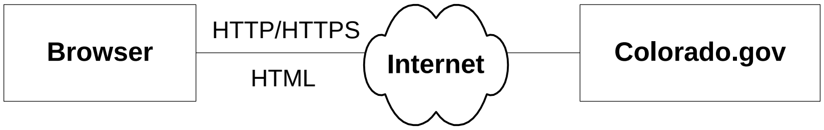


FIGURE 7.3 WEB ACCESS

7.3.1 HyperText Markup Language (HTML)

HTML (HyperText Mark-up Language) interface is the standard for user interfaces. All new development efforts are required to design an HTML interface as the systems primary user interface.

7.3.2 Extensible Markup Language (XML)

XML (Extensible Markup Language) is the standard format for server-to-server data interchange. All new development efforts are required to design XML interfaces, define data interchange documents via Document Type Definitions (DTD), and implement services to accept requests and provide replies to valid DTD's.

7.4 Email

State Email systems must support the following standards:

- Simple Mail Transport Protocol (SMTP),
- Post Office Protocol (POP) and/or Internet Mail Access Protocol (IMAP), and,
- Multipurpose Internet Mail Extensions (MIME)

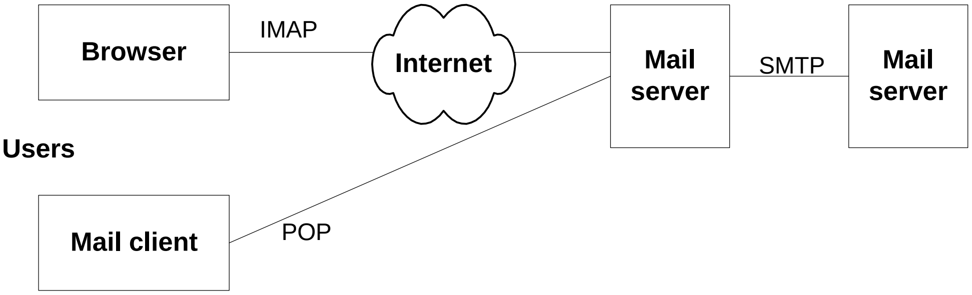


Figure 7.4 Email Architecture

7.4.1 Simple Mail Transport Protocol (SMTP)

SMTP is the standard for exchange of email between servers. All State email servers must support SMTP.

7.4.2 Post Office Protocol (POP) and/or Internet Mail Access Protocol (IMAP)

All State email servers must support POP3 or IMAP4 for client access.

7.4.3 Multipurpose Internet Mail Extensions (MIME)

All State email servers must support MIME content.

7.5 Identity Management

Large number of users, constituents, employees, partners and suppliers are allowed to access systems and information in the State's web enabled enterprise. Identity management is the capability to manage these varied identities and levels of access, across the enterprise's varied environments.

An identity management system must include administrative and self-service interfaces that simplify and automate managing the addition (provisioning) and removal (deprovisioning) of users and their ability to access systems.

Delegated administration allows multiple administrators to assist in the provisioning and management of users, allowing the main administration group to delegate some authority to departments or agencies, as necessary. This allows the large problem of user identity to be divided into manageable pieces.

7.5.1 Directory

A solid directory foundation is required infrastructure necessary to enable mission-critical security and authentication.

7.5.1.1 Lightweight Directory Access Protocol (LDAP)

All State directories must support the LDAP standard.

7.5.1.2 X.500 Directory Services Model

All State directory structures must follow the x.500 standard.

7.6 Database

At the heart of the enterprise architecture is data storage, manipulation, and retrieval. In order to provide a high quality and consistent level of data service within and between agencies, the State will mandate that all new database management system satisfy the following conditions. Database systems that do not meet such standard will at minimum provide gateways that enable their data to be shared by relational systems using SQL as the standard means of interaction.

7.6.1 Open Database Connection / Java Database Connectivity (ODBC/JDBC)

ODBC/JDBC is the standard for database connectivity. All State database systems must provide for ODBC and/or JDBC connections.

7.6.2 Structured Query Language (SQL)

Structured Query Language (SQL) is the standard for database queries. All State database systems must support SQL.

7.6.3 Relational Database Management System (RDBMS)

All State databases must be relational database management systems.

7.6.4 RDBMS Administrator Security

Default accounts that provide administrator or "super user" privileges in an RDBMS shall be protected.

7.6.4.1 Default Administrator Passwords

Default administrator user passwords shall be changed on installation.

7.6.4.2 Administrator Passwords Strongly Formed

Administrator or super-user passwords shall be strongly formed.

- The password must contain at least one number, one lower case character and one uppercase character.
- The password cannot contain any dictionary word greater than or equal to four (4) characters.
- The password cannot be changed to any of the three (3) previous passwords.
- The password must be at least eight (8) characters long.

7.6.4.3 Administrator Passwords Changed Every 90 Days

All administrative passwords shall be changed at least every ninety (90) days, and on departure of any person with knowledge of those passwords.

7.6.4.4 Administrator Password Storage

Administrative passwords shall not be stored anywhere on the file system in text readable format; this includes operational batch scripts, application programs and password files.

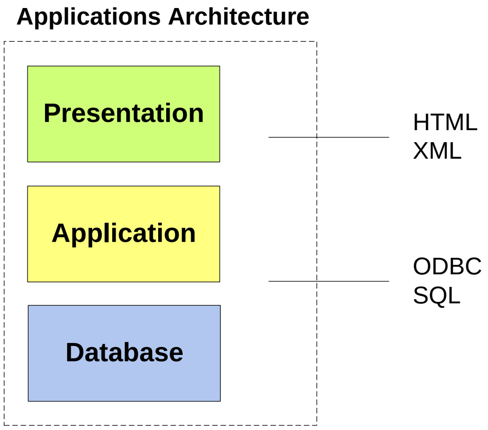
7.6.4.5 Log Failed Admin Access Attempts

All failed attempts to gain access to user accounts with administrative privileges shall be logged and reviewed at least weekly.

7.7 Application

Common application development methodologies ensure consistency of application development and support. Tool-based development enables tool-based operations and support, which improves systems long-term maintainability, reducing total cost of ownership.

Figure 7.7 Application Architecture



7.7.1 n-Tier Application Development

All State web applications shall be developed following the n-tier development model to clearly separate presentation (look and feel), from the application (business logic), from the database.

In addition to the advantages of distributing programming and data throughout a network, n-tier applications have the advantage that any one tier can run on an appropriate processor or operating system platform and independently of the other tiers.

7.7.2 Tool Supported Software Development

All State applications development shall be supported by software engineering tools for the management of requirements, design, and software development.

7.7.3 Analysis and Design

All analysis and design must be performed using generally accepted and disciplined methodology.

7.7.4 Uniform Modeling Language (UML)

Every State application must have accompanying Use Case models, Class Diagrams, Component models, and Deployment Diagram.

7.7.5 Configuration Management

Management of software assets (models, code, documentation, test cases, etc) shall be centralized in a configuration management repository.

7.8 Security

The State has an obligation to its citizens, businesses, employees, and its agencies and departments to provide security of information residing in and traveling to or from state operated computers.

7.8.1 Encryption

All State computational resources using encryption shall use approved encryption algorithms and key lengths. (112 or 168 bit 3DES , 128 bit SSL, or AES – Advanced Encryption Standard) for data in transit as well as data in place. The use of proprietary encryption algorithms is not allowed for any purpose.

7.8.2 Intrusion Detection Service (IDS) – Network Based

All publicly accessible, State computers must have a network based intrusion detection service capable of combating unauthorized intrusions, malicious Internet worms, bandwidth attacks and e-Business application attacks.

The IDS must provide stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection.

The IDS must monitor all IP protocols (e.g. TCP, UDP etc).

The IDS must statefully decode application-layer protocols (e.g. FTP, SMTP, HTTP, DNS, RPC, Telnet etc).

The IDS must interact with firewalls and other network devices to actively shunt attacks and provide event notification.

7.8.3 Virus Detection

All State computers shall have software capable of detecting known viruses and worms and informing system administration personnel which files are infected. This software must allow for periodic update of its virus list from an external source.

7.8.4 Wireless Security

Access to State of Colorado networks via unsecured wireless communication mechanisms is prohibited. Only wireless systems that meet the following criteria are approved for connectivity to State networks.

This standard covers all wireless data communication devices connected to any State internal network. This includes any form of wireless communication device capable of transmitting data. State wireless connections must:

- Maintain point-to-point hardware encryption of at least 128 bits.
- Support strong user authentication which checks against an external database such as TACACS+, or RADIUS.
- 802.11b (Wi-Fi) devices must be LEAP/EAP/PEAP compliant.

7.8.5 DMZ

A DMZ protects internal networks from the public network. A DMZ shall be part of all State systems that allow for access to or from the Public Internet. The DMZ must be hosted in a datacenter (see Section 5.2).

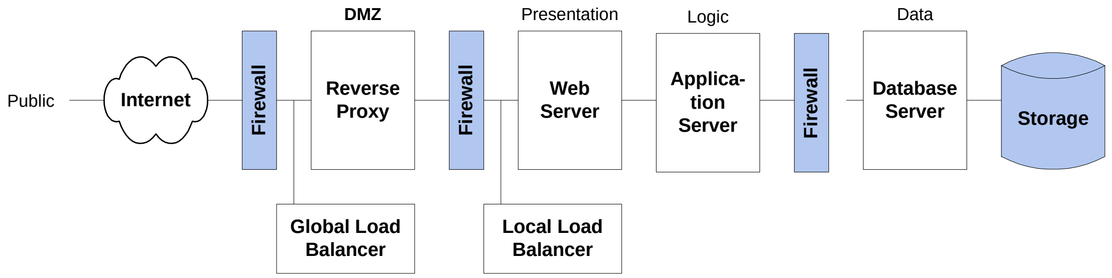


Figure 7.8.5 Three Firewall DMZ

7.8.6 Authentication / Authorization / Accounting

TACACS+, Radius, or Kerberos authentication must be used for access to all State network resources and devices. Access to systems will require 3-element authentication (e.g. an identifier – username, something you know – password, something you have – SecurID code). Roles and privileges must be maintained in an LDAP compliant data store. Access to State computing & networking facilities and devices will be audited by a combination of hardware and software components that determine which persons are using the system.

7.8.7 System Administrator Security

Default accounts that provide administrator, root, or “super user” privileges on computer equipment shall be protected.

7.8.7.1 Default Administrator Passwords

Default administrator passwords shall be changed on installation.

7.8.7.2 Administrator Passwords Strongly Formed

Administrator passwords shall be strongly formed.

- The password must contain at least one number, one lower case character and one uppercase character.
- The password cannot contain any dictionary word greater than or equal to four (4) characters.
- The password cannot be changed to any of the three (3) previous passwords.
- The password must be at least eight (8) characters long.

7.8.7.3 Administrator Passwords Changed Every 90 Days

All administrative passwords shall be changed at least every ninety (90) days, and on departure of any person with knowledge of those passwords.

7.8.7.4 Administrator Password Storage

Administrative passwords shall not be stored anywhere on the file system in text readable format; this includes operational batch scripts, application programs and password files.

7.8.7.5 Log Failed Admin Access Attempts

All failed attempts to gain access to user accounts with administrative privileges shall be logged and reviewed at least weekly.

7.8.8 Web Security

The State shall us HTTPS (SSL) and WS-Security to ensure secure transmission of information to and from the public Internet. SSL provides transport level security. WS-Security provides message level security for web services. WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication.

II. A migration strategy for compliance.

Migration to the above body of established IT standards will be determined as follows:

- All existing systems or systems currently under development will continue to be developed or supported "as is" until their life cycle is close to completion.
- All existing systems, at the end of their life cycle, must be brought up to the new standard.
- All system enhancements and upgrades shall improve standards compliance.
- All new systems and major system enhancements must meet State standards upon implementation.

Chapter 2

Control

Management Rule	**Number**
IT Lifecycle Management Process	2-1
IT Security	2-2
IT Procurement Review	2-3
IT Contingency and Disaster Recovery Planning	2-4

Rule 2-1

IT Lifecycle Management Process

Authority

C.R.S. 24-37.5-106 (1)(e) – Manage IT investments throughout life cycle (OIT)

Definition

IT Project: A temporary endeavor, with a defined start and end date, to create a unique product, service, or result that is undertaken to support one or more objectives of one or more lines of business of state government and requires communication and information resources and/or technologies.

Rule

It is a directive of the Commission on Information Management (IMC), that all state agencies shall report Status on and receive approval before proceeding through the various lifecycle stages of all IT projects through the state’s lifecycle management process.

The State’s IT lifecycle management process shall be comprised of stages and gates including, but not limited to, project definition, procurement, development, implementation, operation, performance evaluation, and enhancement or retirement. This process shall promote multi-level business and technical review of each IT project at appropriate gates.

The IMC/OIT shall periodically review the performance of state agencies in managing their it projects and may, when appropriate, reduce oversight on agency it projects.

Criteria

Progression of initial, continued, and on-going technology investments through the lifecycle management process shall be approved only when it is determined, by the IMC and/or OIT, that they are in alignment and/or compliance with IMC plans, policies, and directives, using criteria including:

- cost
- size
- technical alignment with agency and state plans and existing architecture
- risk
- sourcing of common/shared services

The review forms, content, and due date(s) shall be determined by the IMC, in consultation with agency chief information officers.

Rule 2-2
IT Security

Authority
C.R.S. 24-37.5-106 (1)(c) – Policies, standards, specifications, and guidelines for IT (OIT)
C.R.S. 24-37.5-203 (1)(e) – Oversee on-going use of statewide infrastructure (IMC)
C.R.S. 24-37.5-204 – Status of state agencies (IMC)

Purpose
Security is a mission critical business requirement for all government operations. It is the policy of the State of Colorado to secure and protect the State's information and technology as valuable strategic assets belonging to the people of Colorado.

Definition
Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Rule
It is a directive of the Commission on Information Management (IMC), that each agency develop and implement an information security program and utilize a layered security approach to protect its IT assets. Each agency information security program shall consist of, at a minimum, these eight (8) components:

- business impact analysis that assesses the criticality of services
- risk/security assessment that identifies environment vulnerabilities
- risk management process
- contingency plan for disaster recovery
- identifies Security safeguards for asset protection
- secure architecture design
- developed security awareness and training programs
- monitor/audit system for back end reviews and efficiency/effectiveness analysis.

Further, each agency shall designate an individual to act as an agency Information Security Officer to direct its internal security program as well as collaborate with the State Chief Information Security Officer, IMC, and OIT regarding the current state of the agency's security program and the agency's security needs.

In the event of a security incident, state agencies shall immediately comply with policy directives from the State Chief Information Security Officer with respect to such incident.

The information security program review Form, content, and due date(s) shall be determined by the IMC, in consultation with agency chief information officers.

Rule 2-3
IT Procurement Review

Authority
C.R.S. 24-37.5-101 (1)(d) – Agencies independently acquire technologies (OIT)
C.R.S. 24-37.5-106 (1)(b) – Require agencies to submit plans (OIT)
C.R.S. 24-37.5-106 (1)(g) – Review of IT procurements (OIT)
C.R.S. 24-37.5-106 (1)(h) – Aggregate IT procurements (OIT)
C.R.S. 24-37.5-106 (1)(j) – Outsource resources and services
C.R.S. 24-37.5-202 (1)(e) – Disapprove non-conforming agency procurements (IMC)

Purpose
To coordinate agencies acquisition of communication and information technologies and resources to avoid duplication and maximize cost effectiveness and use.

Definition
IT Procurement: Any acquisition, by one or more state agency for their possession or use, of communication and information technologies and/or resources valued at or above the statutory limit – regardless of funding source (e.g. federal, state, local, private sector funds; or AS an appropriation, grant, gift, revenue) or acquisition mechanism (e.g. agreement, contract, purchase order).

Rule
It is a directive of the Commission on Information Management (IMC), that all state agencies shall:

- submit, to the Governor's Office of Innovation and Technology (OIT), a current annual IT procurement plan; and
- report individual IT procurements to OIT in advance of initiating solicitation or selection of the targeted communication and information technologies and/or resources.

Criteria
Furthermore, the body of IMC plans, policies, and directives shall represent the criteria to be used for approving or rejecting agency procurements. IT procurements shall be approved only when it is determined, by the IMC and/or OIT, that they are in Alignment and/or compliance with all IMC plans, policies, and directives, including:

- annual Department IT Plans
- IT Expenditure Accounting (IT Chart of Accounts)
- IT Lifecycle Management Process
- IT Management Principles
- State's Information and Technology Management Code (IMC Rules)
- State's Strategic Communications and Data Processing plan
- statewide IT Plans
- statewide IT standards

When a proposed IT procurement is submitted to the IMC/OIT for review, the IMC/OIT will have until the close of the fifth business day after receiving said item to either:

a) approve or deny the request; or
b) inform the agency of concerns regarding the request and extend the review period to facilitate further documentation and discussion.

When an IT procurement is rejected, the agency shall be immediately provided with a clear explanation, referencing the criteria above, of the basis for such a decision.

Failure by the IMC/OIT to respond with one of the above actions in the appropriate timeframe shall be considered as an approval of the request.

The review form, content, and due date(s) shall be determined by the IMC, in consultation with agency chief information officers.

Rule 2-4
IT Contingency and Disaster Recovery Planning

Authority

C.R.S. 24-37.5-106 (1)(b) – Require state agencies to submit plans (OIT)
C.R.S. 24-37.5-202 (1)(b) – Assess current state of systems (IMC)
C.R.S. 24-37.5-202 (1)(g) – Study needs of state agencies (IMC)
C.R.S. 24-37.5-203 (1)(b) – Review existing portions of statewide infrastructure (IMC)
C.R.S. 24-37.5-203 (1)(e) – Oversee on-going use of statewide infrastructure (IMC)

Rule

It is a directive of the Commission on Information Management (IMC), that all state agencies shall prepare and test IT contingency and disaster recovery plans that will be maintained and used in the event of degraded or interrupted performance of the communications and information resources and technologies.

Criteria

Furthermore, the IT contingency and disaster recovery plan(s) shall include:

- recovery requirements
- plan administration
- training plan
- testing plan
- communication plan
- recovery procedures
- inventory
- notification procedures
- team structure

The chief information officer of each agency shall annually certify to the IMC as to their agency's compliance with this rule. The certification form, content, and due date(s) shall be determined by the IMC, in consultation with agency chief information officers.

Chapter 3

Evaluate

Management Rule	**Number**
IT Expenditure Accounting	3-1
Systems Documentation	3-2

Rule 3-1
IT Expenditure Accounting

Authority

C.R.S. 24-37.5-106 (1)(g) – Review of it procurements (OIT)
C.R.S. 24-37.5-202 (1)(e) – Disapprove non-conforming agency procurements (IMC)
C.R.S. 24-37.5-203 (1)(d) – System to manage use of statewide network (IMC)

Definition

IT Chart of Accounts: The subset, from the State's centrally defined Chart of Accounts (managed by the State Controller's Office), of expenditure object codes designated (by the Commission on Information Management) for reporting spending on communication and information technologies and resources.

IT Expenditure: Any purchase or disbursement or payment of money, by one or more state agency, for communications and information resources and/or technologies – regardless of funding source (e.g., federal funds, grant, state appropriation) or acquisition mechanism (e.g., agreement, contract, purchase order). An expenditure is made when the actual spending occurs or when there is a contractual agreement requiring such spending and the amount is determined.

Rule

It is a directive of the Commission on Information Management (IMC), that each and every IT expenditure, upon being entered into the State's financial system, shall be coded with the most appropriate IT expenditure object code from the State's IT Chart of Accounts.

The State's IT Chart of Accounts is composed of several categories (e.g., hardware, services, software) and sub-categories (e.g., capitalized vs. non-capitalized, leased vs. purchased).

The IMC will provide recommendations to the State Controller's Office for the IT Chart of Accounts' framework and content.

Rule 3-2
IT Systems Documentation

Authority

C.R.S. 24-37.5-106 (1)(b) – Require state agencies to submit plans (OIT)
C.R.S. 24-37.5-106 (1)(e) – Effective management of IT investments (OIT)
C.R.S. 24-37.5-106 (1)(i) – Efficient exchange of information and technology (OIT)
C.R.S. 24-37.5-202 (1)(b) – Assess current of systems (IMC)
C.R.S. 24-37.5-202 (1)(g) – Study needs of state agencies (IMC)
C.R.S. 24-37.5-203 (1)(b) – Review existing portions of statewide infrastructure (IMC)
C.R.S. 24-37.5-203 (1)(e) – Oversee on-going use of statewide infrastructure (IMC)

Purpose

Communication and information resources in the various agencies of state government are valuable strategic assets belonging to the people of Colorado that must be managed accordingly. The sharing of communication and information resource technologies among agencies is often the most cost-effective method of providing the highest quality and most timely governmental services that would otherwise be cost prohibitive.

Definition

IT System: An assemblage of inter-related IT architecture components designed to work as a coherent entity. Communication and information technologies and resources connected together in order to facilitate the flow of information serving a common purpose. Information and technology elements which automate a unified set of business processes.

Architecture Stack

Interface
Application
Data
Staff
Computing Platform
Network
Facility

Rule

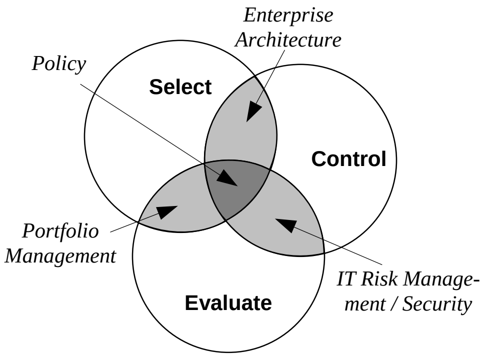
It is a directive of the Commission on Information Management (IMC) that all state agencies shall develop and submit regularly on at least an annual basis, to the IMC and/or OIT, current documentation that profiles each IT system.

The documentation form, content, and due date(s) shall be determined by the IMC, in consultation with agency chief information officers.

Commission on Information Management
225 E 16th Avenue, Suite 260
Denver, Colorado 80203-1606

Phone: 303-866-6060
Fax: 303-866-6454

www.colorado.gov/oit


Enterprise Architecture
Policy
Select
Control
Portfolio Management
Evaluate
IT Risk Management / Security